

Serial No. 09/269,618

**Remarks**

The various parts of the Office Action (and other matters, if any) are discussed below under appropriate headings.

**I. Interview Summary**

In a telephone interview on November 2, 2004, the undersigned, the Inventor, and the Examiner discussed the differences between the claimed invention, particularly claim 1, and the prior art, particularly Hiroya et al. (U.S. Patent No. 5,754,654) and Rosen (U.S. Patent No. 5,898,154). No agreement was reached. The undersigned thanks the Examiner for his time.

**II. Claim Rejections - 35 USC § 102 and § 103**

Claims 1, 3-48, 51-53, 61-63, 65-69 and 74 have been rejected under § 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,898,154 to Rosen ("Rosen") in view of U.S. Patent No. 5,754,654 to Hiroya et al. ("Hiroya") and further in view of Schneier's Applied Cryptography, Second Edition ("Schneier").

Claims 1 and 61-63 have been amended to incorporate the redemption instruction information feature, which can be found in claims 13 and 52, for example. New claims 75-78 have been added. The undersigned respectfully submits that the rejected claims are not unpatentable over the applied references for at least the following reasons.

**A. Rosen fails to teach or suggest the claimed first, third and redemption instruction information**

Rosen discloses a monetary system that uses electronic notes 11 that act as cash. These notes can be freely transferred from one registered subscriber to the system to another subscriber without returning the electronic note to an issuer for each transaction. Consequently a chain or tree of transferee signatures can accumulate in Rosen's electronic notes, just like a paper check, before the electronic note is redeemed. At any point in time, the note might have been double spent, making it worthless if someone else has already presented a copy of the electronic note to an issuer for redemption. Rosen tries to overcome this limitation by requiring users of the system to subscribe and to use tamper-resistant hardware for transferring the electronic

Serial No. 09/269,618

notes.<sup>1</sup> The disclosed invention is not limited to subscribers and does not require the use of tamper-resistant hardware.

Turning to the claims, the Examiner has taken the position that the claimed value note reads on Rosen's electronic note 11, the claimed first information reads on Rosen's identifier for money generator module 6, the claimed issuer's signature and issuer's public key information reads on Rosen's issuing bank's identifier (column 14, lines 6-14), the claimed redemption instruction information reads on Rosen's Body Group of data fields (column 19, lines 30-65) and the claimed bearer's signature reads on Rosen's digital signature of the Money Generator module 6 (column 19, lines 54-67 and column 20, lines 1-4).<sup>2</sup>

The applicant respectfully disagrees. First, the value note of the claimed invention does not read on Rosen's electronic note 11 because Rosen's electronic note 11 lack the first and third information of the claimed invention. The data fields that make up element 11 are listed in column 19, lines 34-60. Rosen's electronic notes 11 are generated at a Money Generator module 6 by an issuing bank 12, and the value of each note is signed.<sup>3</sup> At the time that this signature is made, the note is still at the bank, so this signature only signs the Body Group of data and is unable to sign any bearer information (which is part of Rosen's Transfer Group data). The Transfer Group data is formed only after the first transaction of the note.<sup>4</sup>

The bearer's public key information also does not read on the identifier for Rosen's Money Generator module as stated by the Examiner. The claimed bearer's public key represents the bearer who obtains a value note from the issuer. The bearer's public key is used to authenticate the bearer when the note is returned to the issuer for redemption or transfer. The Money Generator module "generates the electronic money" and accordingly is the issuer rather than the bearer.<sup>5</sup> Therefore, the

---

<sup>1</sup>See Rosen, col. 10, line 51 through col. 11, line 3.

<sup>2</sup>Office Action dated June 2, 2004, page 4.

<sup>3</sup>See Rosen, FIG. 6.

<sup>4</sup>See Rosen, col. 19, lines 47-53.

<sup>5</sup>Rosen, col. 16, lines 62 and 63.

Serial No. 09/269,618

electronic note 11 does not contain a public key that represents a bearer that is signed by the issuer.

The Transaction money module in Rosen more closely resembles the bearer in the claimed invention. The electronic note 11, however, does not contain any data field that represents a public key of the Transaction money module until after the first transaction after issuance. Since Rosen does not return the note 11 to the issuer for each transaction, the issuer cannot sign the Transaction money module's public key.

In fact, Rosen does not sign any information that can be used to authenticate that an electronic note was sent from a particular Transaction money module. Instead, Rosen signs identifying information for the Money Generator module which functions as the issuer rather than the bearer. Consequently, Rosen does not utilize the relationship between the first and third information found in the claims.

Another difference between a value note in accordance with the claimed invention and Rosen's electronic note 11 is explained by the way the differing systems are used. For the claimed value note, the first information allows an issuer to verify whether the note is being redeemed by the correct bearer. This is similar to the way paper checks are redeemed. To ensure that a check is tendered by the correct bearer, the bank requires the bearer to sign the check. The bearer's signature is then verified. Similarly, in the claimed invention the bearer's public key is used to authenticate the bearer and the bearer's public key is signed by the issuer to ensure that the bearer's public key and the second information (e.g., the amount of money represented by the value note) has not been altered between issuance and redemption.

In contrast, Rosen's electronic note 11 is used more like cash than a check. Rosen's electronic notes can be freely transferred without asking an issuer to verify the bearer in each transaction. In Rosen's system it is sufficient to know that the electronic note was issued by a valid Money Generator module, a valid issuer, because any further transactions will occur between registered subscribers using tamper-resistant Transfer money module hardware. Therefore, Rosen signs the identifying information of the Money Generator module, the issuer rather than a bearer.

From the Money Generator module, the note passes to a Transfer Money Module, the buyer (the first bearer). When the buyer wants to pay a vendor, the buyer (the bearer) appends the buyer's signature to the end of the Transfer Group data and passes the note to the vendor (the new bearer). At the time the vendor receives the

Serial No. 09/269,618

note, the vendor relies on the buyer, presumably a subscriber using a tamper-resistant Transfer Money module, and the bank's Money Generator module, the issuer. If the buyer (or anyone else in the chain of title (the transaction list in the Transfer Group data) has already spent this note, it will be worthless when the vendor presents it to the bank (the issuer) for redemption. Although the bank could quickly determine the guilty party when a second copy of the electronic note is presented for redemption, the vendor's only recourse is with the buyer who presented the electronic note.

Consequently, when the buyer signs the note, it is not a guaranteed redemption of the original note. The buyer does not lose the ability to sign the note again and again, passing it to multiple vendors. Likewise, when the vendor goes to the bank to redeem the note, the vendor's signature is not a guaranteed redemption of the note, since the bank will redeem the first instance in which the note is presented for redemption, which could be by another vendor if the note was double spent by a bearer. Rosen tries to overcome this problem by requiring subscribers and having the subscribers use tamper-resistant units as Transfer Money modules.<sup>6</sup> An advantage of the claimed invention is that the issuer's signature authenticates the value note to any future bearer.

Yet another difference is that the claimed value notes must be returned to the issuer for each transfer. The issuer can issue a new value note wherein the bearer's public key in the first information is changed to represent the new bearer before a new value note can be issued. (See claims 20, 22, 24 and 41, 43, 45, for example.)

Furthermore, this first information is signed by the issuer to ensure it is not altered after the value note is issued. When being transferred, the issuer creates a new value note with new first information that represents the new bearer so that new bearer can be authenticated when they subsequently either redeem or transfer the value note.

No teaching or suggestion of redemption instructions to the issuer have been found in Rosen. Rosen's Transfer Group data simply lists a chain of transactions, not redemption instructions.

Rosen also describes electronic credit notes, as opposed to currency notes, that can only be transferred by the owner of the account, similarly to how the claimed value notes can only be transferred from the original bearer. These electronic credit notes,

---

<sup>6</sup> Rosen, col. 10, lines 50-60.

Serial No. 09/269,618

however, still lack data similar to the claimed first and third information. The account number identifier that identifies the account owner and recipient of Rosen's electronic credit note is different from the first information of the claimed invention. Rosen's account number is not in the form of a public key and therefore cannot provide authentication that the actual account holder transferred the electronic credit note. The claimed value note's first information can ensure that the bearer seeking redemption is the actual bearer to whom the value note was issued, because the issuer can verify the bearer's public key, and the issuer has signed the bearer's public key.

#### **B. Hiroya fails to overcome Rosen's deficiencies**

Like Rosen, Hiroya provides for a means of payment that can be transferred from one bearer to another, but Hiroya's electronic tickets do not accumulate a chain of signatures. Instead, Hiroya relies on special hardware devices to make sure that overspending does not occur.<sup>7</sup>

Hiroya discloses an electronic ticket vending system that uses dedicated hardware to conduct ticket transactions. The Examiner has taken the position that the claimed value note reads on Hiroya's electronic ticket storage device, the claimed first information reads on Hiroya's PTi, and the claimed step of calculating third information reads on Hiroya's STk in Hiroya's column 15, lines 38-44.<sup>8</sup>

Hiroya fails to redress Rosen's deficiencies. To begin with, the first information of the claimed invention does not read on PTi or any other aspect of Hiroya. Even though the claimed first information and Hiroya's PTi both are related to "public" keys, they serve completely different functions within the respective inventions and their similarities end with their names.

In the disclosed first information, the bearer's public key is utilized for authentication purposes, specifically, "to verify whether the bearer's signature is correct when the value [note] is redeemed."<sup>9</sup> In general, authentication makes sure the value note is provided by the bearer who claims to be sending it. Therefore, the public key

---

<sup>7</sup>See Hiroya, col. 10, lines 55-60.

<sup>8</sup>Office Action dated June 2, 2004, page 3.

<sup>9</sup>Specification, page 6, lines 11 and 12.

Serial No. 09/269,618

allows the issuer (such as a bank) to verify that a particular value note is being redeemed by the original bearer, the bearer to whom it was issued.

In Hiroya, however, PTi is a "public" key that is utilized for encryption purposes rather than authentication. Encryption also provides security to the system but not in the same way authentication does. Generally, encryption translates data into an undecipherable form so that the encrypted data is not read by unauthorized individuals. As explained in Hiroya, PTi is actually used to decrypt the message sent between the electronic ticket storage device and the electronic ticket vending and refunding device.<sup>10</sup> The actual ticket data, transaction identification, and transaction sequence number are included in a message R. R is encrypted by the local secret key before being sent by the electronic ticket storage device. On the receiving side, the electronic ticket vending and refunding device decrypts "the message R using the public key PT12." (PT12 being a specific instance of PTi).<sup>11</sup> Therefore, the claimed first information and Hiroya's PTi clearly serve distinctive purposes in their respective systems. The claimed first information is used for authentication while Hiroya's PTi is used for decryption. Consequently, applicant's first information does not read on PTi.

Another feature present in the claimed invention and lacking in Hiroya and Rosen is the relationship between the first and third information. This relationship ties together the ability to authenticate a value note and also to ensure that the value note was not altered.

In the claimed invention, the issuer's key is used to "sign" the data of the value note. The issuer's signature represents the third information. In Hiroya, the secret key, STk, is used to "sign" the ticket information data.<sup>12</sup> The difference is that in the claimed invention the first information discussed above is included in the signed information. In contrast, Hiroya fails to "sign" data equivalent to the bearer's public key, which is part of the claimed first information. Consequently, in the claimed invention the bearer's public key is part of the signed information. The issuer's signature ensures that the bearer's public key and the second information have not been altered since the note was issued. In Hiroya, only the ticket information data is signed. The ticket information data includes "a ticket publication source, an event name, a day and time, a place name, a

---

<sup>10</sup>See generally, Hiroya, columns 16 and 17.

<sup>11</sup>Hiroya, column 17, lines 14 and 15.

<sup>12</sup>See Hiroya, column 15, line 44.

Serial No. 09/269,618

seat number, and a serial number."<sup>13</sup> Therefore, Hiroya's signature can only be used to verify that the ticket information data has not been altered. Unlike the claimed third information, Hiroya's signed information does not include a public key that can be used for authentication purposes.

No teaching or suggestion of redemption instruction information has been found in Hiroya either. The Examiner took the position that Hiroya's message VR reads on the claimed redemption instruction information.<sup>14</sup> But instead of redemption instruction information, VR is produced "from the message R, the ticket information, and the electronic signature."<sup>15</sup>

Rosen describes a situation where a vendor transacts with a buyer who transmits PT12\*STg+VR\*ST12. PT12\*STg is a signed version of PT12 by g (the signature of a global certification agency). This signature verifies PT12. Unlike the claimed value notes, however, this signature signs no second information (e.g., money value). Thus, the second information is not tied to a public key. The certification of PT12 is necessary in Rosen to tie PT12 to the secured hardware device that protects the system.<sup>16</sup>

The remaining portion VR\*ST12 is a signed transaction consisting of an amount V and a message identifier R provided by the vendor, and signed by the buyer when paying for the ticket. This signature is not a redemption that can be traced back to redeem a particular sum of money issued by the bank. Instead, like a blank check this signature can sign any arbitrary sum, since V was never signed by an issuer (such as a bank), only the payer.

Consequently, at the time the vendor receives this message, there is no way for the vendor to determine whether ST12's account is already overdrawn, and must trust the hardware device that contains ST12. Only the hardware device prevents overspending. Since all hardware devices have their own PT12\*STg, anyone who can extract ST12 from a device can produce limitless messages in the form

---

<sup>13</sup>Hiroya, column 15, lines 31-34.

<sup>14</sup>Office Action dated June 2, 2004, page 4, citing Hiroya, column 4, lines 24-28.

<sup>15</sup>Hiroya, column 20, lines 24-26.

<sup>16</sup>Hiroya, col. 18, lines 60-65.

Serial No. 09/269,618

PT12\*STg+VR\*ST12, and produce limitless amounts of money. This explains why Hiroya's system only operates with special hardware devices.<sup>17</sup>

Hiroya's system cannot overcome this limitation, since at the time of the communication it is not in communication with the global certification authority, g.<sup>18</sup> Moreover, PT12\*STg+VR\*ST12 also does not include the vendor's public key, PT11, whereas the claimed invention includes the bearer's public key, certified by the issuer's secret key.<sup>19</sup>

**C. Schneier also fails to overcome the deficiencies of Rosen and Hiroya**

The third reference, Schneier, also fails to overcome the deficiencies of Rosen and Hiroya. Schneier shows that Hiroya reverses the traditional usage of the terminology for public and private keys. The Examiner's position goes further than Schneier, suggesting that a public/private key could be used for both encryption/decryption and digital signature purposes.<sup>20</sup> Traditionally, public keys are used for encryption and private keys are used for decryption.<sup>21</sup> This is because public keys are not kept secret, as suggested by their name. Thus, designing a system that allows unauthorized parties to use a public key to decrypt a message is counterintuitive. Therefore, the traditional method is to encrypt a message with a public key that is widely available, and enable only those with the secret key to decrypt the message.

Hiroya describes using secret keys to encrypt the message and the public keys to decrypt the message. In preparing an electronic ticket for transmittal, for example, Hiroya's electronic ticket vending and refunding device encrypts a public key, PT12, with a secret key, STg, and encrypts the message, R, with a secret key ST12.<sup>22</sup> On the receiving side, the electronic ticket storage device uses public keys to decrypt the

---

<sup>17</sup>See Hiroya, col. 18, lines 60-65.

<sup>18</sup>Hiroya, col. 16, line 49.

<sup>19</sup>See Hiroya, col. 19, lines 30-46.

<sup>20</sup>Office Action dated June 2, 2004, page 4.

<sup>21</sup>See Schneier, page 31.

<sup>22</sup>See Hiroya, column 17, line 8.



Serial No. 09/269,618

transmitted electronic ticket.<sup>23</sup> Therefore, an intercepted transmission could be decrypted by anyone with the public keys, which presumably would be readily available to the public. Hiroya clearly states that each ticket storage device retains the global public key, PTg, for decryption.<sup>24</sup> This enables each ticket storage device could decrypt any electronic ticket. This is why secret keys are traditionally used for decryption, to ensure that only authorized parties with secret keys can decrypt a message.

Consequently, it would not have been obvious to one of ordinary skill in the art at the time of the invention to combine "Hiroya/Rosen/Schneier" as suggested in the Office Action. In contrast, it would be rather surprising for one of ordinary skill in the art to follow such a counterintuitive method of using public and private keys.

In summary, the third information of the claimed invention includes a signature which signs the first information containing the bearer's public key. The public key is used for authentication and ensures the value note is provided by the actual bearer who claims to be sending it, while the signature ensures that the public key in the first information is not altered. This intertwined relationship between the first information and the third information enhances both authentication and the ability to ensure that the public key has not been altered. Hiroya has no such relationship between an electronic signature and a public key. First, PTi is used for decryption rather than authentication. Second, the electronic signature in Hiroya is only used to sign the ticket information data, rather than any data that could verify the bearer of a ticket. Therefore, claim 1 does not read on Hiroya

#### D. Conclusion

In conclusion, the claimed invention utilizes the bearer's public key and the issuer's digital signature in an interlocking manner that provides a very secure method of issuing value notes that is not present in either Hiroya or Rosen or Schneier. The interlocking manner between the first and third information provides for secure authentication, by the issuer, of the original bearer of a value note, and also provides the ability to ensure that the public key used for authentication, as well as additional information, has not been altered. Moreover, redemption instruction information has

---

<sup>23</sup>See Hiroya, column 17, lines 12-15.

<sup>24</sup>See Hiroya, column 16, lines 45 and 46.

Serial No. 09/269,618

not been found to be part of the notes described by Hiroya or Rosen or Schneider. Withdrawal of the rejection is respectfully requested.

In view of the foregoing, request is made for timely issuance of a notice of allowance.

**III. Request for Interview**

If the application is not in condition for allowance, the undersigned requests another telephone interview to further discuss the claims in view of the applied references.

Respectfully submitted,

RENNER, OTTO, BOISSELLE & SKLAR, LLP

By   
Christopher B. Jacobs, Reg. No. 37,853

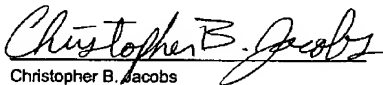
1621 Euclid Avenue  
Nineteenth Floor  
Cleveland, Ohio 44115  
(216) 621-1113

Z:\SEC152\152\DWBYOU\APP0185\PO185US.R09.wpd

**CERTIFICATE OF FACSIMILE TRANSMITTAL**

I hereby certify that this paper, and any documents referred to as attached or enclosed, is being facsimile transmitted to the Patent and Trademark Office (fax no. 703-305-7687) on the date shown below.

Date: December 2, 2004

  
Christopher B. Jacobs